

Multipartite entangled states, symmetric matrices and error-correcting codes

Keqin Feng

Department of Mathematical Sciences, Tsinghua University, Beijing, China

Lingfei Jin*

*Shanghai Key Laboratory of Intelligent Information Processing,
School of Computer Science, Fudan University, Shanghai 200433, China*

Chaoping Xing and Chen Yuan

School of Physical & Mathematical Sciences, Nanyang Technological University, Singapore

(Dated: November 26, 2015)

A pure quantum state is called k -uniform if all its reductions to k -qudit are maximally mixed. We investigate the general constructions of k -uniform pure quantum states of n subsystems with d levels. We provide one construction via symmetric matrices and the second one through classical error-correcting codes. There are three main results arising from our constructions. Firstly, we show that for any given even $n \geq 2$, there always exists an $n/2$ -uniform n -qudit quantum state of level p for sufficiently large prime p . Secondly, both constructions show that their exist k -uniform n -qudit pure quantum states such that k is proportional to n , i.e., $k = \Omega(n)$ although the construction from symmetric matrices outperforms the one by error-correcting codes. Thirdly, our symmetric matrix construction provides a positive answer to the open question in [23] on whether there exists 3-uniform n -qudit pure quantum state for all $n \geq 8$. In fact, we can further prove that, for every k , there exists a constant M_k such that there exists a k -uniform n -qudit quantum state for all $n \geq M_k$. In addition, by using concatenation of algebraic geometry codes, we give an explicit construction of k -uniform quantum state when k tends to infinity.

I. INTRODUCTION

Quantum entanglement appears in many areas of quantum information theory including quantum communications [1–3], quantum computing [4–6] and quantum key distribution [7]. Quantum entanglement theory is developed to determine which states are entangled and which are separable. In bipartite entanglement, the simplest is quantum bipartite pure state. To determine whether this pure state is separable, we just diagonalize its reduced density matrix. But it is still NP-hard to determine separability in bipartite system [8]. In general problem of multipartite entanglement, besides separability and entanglement, there are many types of partial separability which complicates this problem. Although there are some attempts to detect genuine multipartite entanglement [9, 10], there are still many open problems in this area.

One of the intriguing problem is to investigate highly entangled states of several qubits [11–19]. In [20, 21], they considered the one qubit reduced state which is maximally mixed. This idea was further developed by Arnaud and Cerf [22]. They proposed the concept of k -multipartite maximally entangled pure states or k -uniform for short, i.e., any k -partite reduced state is maximally mixed.

It was shown in [29] that an n -qudit pure quantum state $|\Phi\rangle$ of level d is k -uniform if and only if $|\Phi\rangle$ is a

pure $((n, 1, k+1))_d$ quantum error-correcting code. Using this connection the author was able to construct some k -uniform pure quantum states through stabilizer quantum codes obtained from classical self-dual codes. In [23], a connection between k -uniform pure quantum states and orthogonal arrays was established and several classes of k -uniform states were constructed. More precisely speaking, the following result were obtained in [23].

- There exist k -uniform $(d+1)$ -qudits states of d levels whenever $d \geq 2$ and $k \leq \frac{d+1}{2}$.
- There exist 2-uniform n -qudits states of 2 levels whenever $n \geq 5$.
- There exist 3-uniform $(2^m + 2)$ -qudits states of 2^m levels whenever $m \geq 2$.
- There exist $2^m - 1$ -uniform $(2^m + 2)$ -qudits states of 2^m levels whenever $m = 2$ or 4.

In addition, some k -uniform n -qudits states of d levels were also given for some small values of k, n, d . The above special values of the parameters k, n, d are obtained due to constraint from combinatorial structure of orthogonal arrays.

In this paper, we first provide an equivalent definition for k -uniform quantum states through a map from \mathbb{Z}_d^n to the complex numbers \mathbb{C} . Based on this equivalent definition, we first derive a construction of k -uniform quantum states by using symmetric matrices. Again starting from this equivalent definition, we present the second construction that makes use of classical error-correcting codes with good minimum distance and dual distance. There

* lfjin@fudan.edu.cn

are three main results arising from our constructions. Firstly, we show that for any given even $n \geq 2$, there always exists an $n/2$ -uniform n -qudit quantum state of level p for sufficiently large prime p . Secondly, both constructions show that there exist k -uniform n -qudit pure quantum states such that k is proportional to n , i.e., $k = \Omega(n)$ although the construction from symmetric matrices outperforms the one by error-correcting codes. Thirdly, our symmetric matrix construction provides a positive answer to the open question in [23] on whether there exists 3-uniform n -qudit pure quantum states for all $n \geq 8$. In fact, we can further prove that, for every k , there exists a constant M_k such that there exists a k -uniform n -qudit quantum state for all $n \geq M_k$. In addition, by using concatenation of algebraic geometry codes, we give an explicit construction of k -uniform quantum state when k tends to infinity. Both numeric and theoretic results reveal that the matrix construction is in general better than the one by classical error-correcting codes.

The paper is organized as follows. In Section 2, we introduce basic definition of k -uniform quantum states and present an equivalent definition. By this equivalent definition, we propose two different constructions of k -uniform quantum states in Section 3. In Section 4, we investigate the case where n is small by presenting some tables and a few other results. In the last section, we discuss the case where n tends to infinity, i.e., its asymptotic behavior through our construction. In addition, in this section we also provide an explicit construction of k -uniform quantum states based on our construction through error-correcting codes.

II. PRELIMINARIES ON k -UNIFORM QUANTUM STATE

A. Definition

A k -uniform n -qudit quantum state has the property that, after tracing out all but k qudits, we are left with the maximally mixed state for any k -tuple of qudits. This means that all information about the system is lost after removal of $n - k$ or more parties. Precisely speaking, a pure quantum state of n subsystems of level d is called k -uniform (or k -maximally entangled) if every reduction to k qudits is maximally mixed. Let us give a mathematical definition.

The density matrix of a quantum state $|\Phi\rangle = \sum_{\mathbf{c} \in \mathbb{Z}_d^n} \phi_{\mathbf{c}} |\mathbf{c}\rangle$ is defined by $\rho := \sum_{\mathbf{c}, \mathbf{c}' \in \mathbb{Z}_d^n} \phi_{\mathbf{c}} \bar{\phi}_{\mathbf{c}'} |\mathbf{c}\rangle \langle \mathbf{c}'|$. For a subset A of $\{1, 2, \dots, n\}$ and a vector $\mathbf{c} \in \mathbb{Z}_d^n$, we denote by \mathbf{c}_A the projection of \mathbf{c} at A . The reduction of $|\Phi\rangle$ to A has the density matrix $\rho_A := \sum_{\mathbf{c}, \mathbf{c}' \in \mathbb{Z}_d^n} \phi_{\mathbf{c}} \bar{\phi}_{\mathbf{c}'} |\mathbf{c}_A\rangle \langle \mathbf{c}'_A|$, where \bar{A} is the complement set of A (i.e., $\bar{A} = \{1, 2, \dots, n\} \setminus A$) and $\langle \mathbf{c}_A | \mathbf{c}'_A \rangle$ is defined to be 1 if $\mathbf{c}_A = \mathbf{c}'_A$ and 0 otherwise.

Definition 1. A pure quantum state $|\Phi\rangle = \sum_{\mathbf{c} \in \mathbb{Z}_d^n} \phi_{\mathbf{c}} |\mathbf{c}\rangle$ is called k -uniform if for any subset A of $\{1, 2, \dots, n\}$, the reduction of $|\Phi\rangle$ to A has the density matrix $\rho_A = \alpha_A \sum_{\mathbf{c}_A \in \mathbb{Z}_d^k} |\mathbf{c}_A\rangle \langle \mathbf{c}_A|$, where $\alpha_A \in \mathbb{C}$ depends only on A and $|\Phi\rangle$.

Example 1. Consider 5-qudit quantum state of level 2

$$|\Phi\rangle = -|00000\rangle + |01111\rangle - |10011\rangle + |11100\rangle \\ + |00110\rangle + |01001\rangle + |10101\rangle + |11010\rangle.$$

Let $A = \{3, 4\}$. Then an easy computation shows that the density matrix ρ_A is $2|00\rangle\langle 00| + 2|01\rangle\langle 01| + 2|10\rangle\langle 10| + 2|11\rangle\langle 11|$. One can also verify that the density matrix ρ_A has the same form for all other subsets A with $|A| = 2$. By definition, $|\Phi\rangle$ is 2-uniform.

The well-known Greenberger-Horne-Zeilinger states belong to the class 1-uniform, while W states do not belong to any class of k -uniform states. For a state $|\Phi\rangle$, a multipartite entanglement measures $Q_k(|\Phi\rangle)$ was defined [29]. The original Meyer-Wallach measure $Q_1(|\Phi\rangle)$ is actually the average entanglement between individual qudits and the rest. As k increases, $Q_k(|\Phi\rangle)$ is getting more sensitive to correlations of an increasingly global nature. $Q_k(|\Phi\rangle)$ is upper bounded by 1. It was proved in [29, Proposition 2] that $|\Phi\rangle$ is k -uniform if and only if $Q_k(|\Phi\rangle) = 1$.

B. An equivalent definition

An n -qudit quantum state $|\Phi\rangle = \sum_{\mathbf{c} \in \mathbb{Z}_d^n} \phi_{\mathbf{c}} |\mathbf{c}\rangle$ of level d is associated with a map φ from \mathbb{Z}_d^n to \mathbb{C} given by $\varphi(\mathbf{c}) = \phi_{\mathbf{c}}$. This means that n -qudit quantum states of level d are identified with maps from \mathbb{Z}_d^n to \mathbb{C} . Thus, an n -qudit state $|\Phi\rangle$ can be written as $\sum_{\mathbf{c} \in \mathbb{Z}_d^n} \varphi(\mathbf{c}) |\mathbf{c}\rangle$ for a given function φ . A k -uniform quantum state can be described in terms of its associated map φ .

Lemma 1. An n -qudit state $|\Phi\rangle = \sum_{\mathbf{c} \in \mathbb{Z}_d^n} \varphi(\mathbf{c}) |\mathbf{c}\rangle$ is k -uniform if and only if

- (i) φ is not identical to zero.
- (ii) For any subset A of $\{1, 2, \dots, n\}$ with $|A| = k$, and every $c_A, c'_A \in \mathbb{Z}_d^k$, one has

$$\sum_{\mathbf{c}_{\bar{A}} \in \mathbb{Z}_d^{n-k}} \overline{\varphi(c_A, \mathbf{c}_{\bar{A}})} \varphi(c'_A, \mathbf{c}_{\bar{A}}) = \begin{cases} 0, & \text{if } c_A \neq c'_A, \\ \frac{\langle \Phi | \Phi \rangle}{d^k}, & \text{if } c_A = c'_A. \end{cases}$$

Proof. If $|\Phi\rangle$ is k -uniform, by tracing out any $n - k$ qudits, the k -qudit reduced density matrix is proportional to identity matrix. We fix a subset A of $\{1, 2, \dots, n\}$ with $|A| = k$. An n -qudit state $|\Phi\rangle = \sum_{\mathbf{c} \in \mathbb{Z}_d^n} \varphi(\mathbf{c}) |\mathbf{c}\rangle$ is written as

$$|\Phi\rangle = \sum_{\mathbf{c}_A \in \mathbb{Z}_d^k, \mathbf{c}_{\bar{A}} \in \mathbb{Z}_d^{n-k}} \varphi(\mathbf{c}_A, \mathbf{c}_{\bar{A}}) |\mathbf{c}_A\rangle |\mathbf{c}_{\bar{A}}\rangle.$$

Denote by ρ the density matrix of $|\Phi\rangle$, i.e., $\rho = |\Phi\rangle\langle\Phi|$. Consider the reduced state

$$\begin{aligned}\rho_A &= \text{Tr}_{\bar{A}}(\rho) \\ &= \sum_{\mathbf{c}_A, \mathbf{c}'_A \in \mathbb{Z}_d^k} |\mathbf{c}_A\rangle\langle\mathbf{c}'_A| \sum_{\mathbf{c}_{\bar{A}}, \mathbf{c}'_{\bar{A}} \in \mathbb{Z}_d^k} \overline{\varphi(c_A, c_{\bar{A}})} \varphi(c'_A, c'_{\bar{A}}) \langle\mathbf{c}_{\bar{A}}|\mathbf{c}'_{\bar{A}}\rangle \\ &= \sum_{\mathbf{c}_A, \mathbf{c}'_A \in \mathbb{Z}_d^k} |\mathbf{c}_A\rangle\langle\mathbf{c}'_A| \sum_{\mathbf{c}_{\bar{A}} \in \mathbb{Z}_d^k} \overline{\varphi(c_A, c_{\bar{A}})} \varphi(c'_A, c_{\bar{A}})\end{aligned}$$

Since $|\Phi\rangle$ is k -uniform, the reduced state ρ_A is proportional to identity matrix. The sum of diagonal element of ρ_A is $\langle\Phi|\Phi\rangle$ which implies that

$$\sum_{\mathbf{c}_A \in \mathbb{Z}_d^{n-k}} \overline{\varphi(c_A, c_{\bar{A}})} \varphi(c'_A, c_{\bar{A}}) = \begin{cases} 0, & \text{if } c_A \neq c'_A, \\ \frac{\langle\Phi|\Phi\rangle}{d^k}, & \text{if } c_A = c'_A. \end{cases}$$

Vice versa, we have the desired result. \square

III. CONSTRUCTIONS OF k -UNIFORM QUANTUM STATES

Before starting our first construction, we prove a lemma.

Lemma 2. *Let $d \geq 2$ be an integer. Let a_1, a_2, \dots, a_m be m integers. Assume that $\gcd(a_1, a_2, \dots, a_m, d) = e < d$. Then for every $b \in \mathbb{Z}_{d/e}$ the equation $a_1x_1 + a_2x_2 + \dots + a_mx_m \equiv be \pmod{d}$ has exactly ed^{m-1} solutions in \mathbb{Z}_d^m .*

Proof. For $b \in \mathbb{Z}_{d/e}$, we denote by N_b the number of solutions $\mathbf{x} = (x_1, x_2, \dots, x_m) \in \mathbb{Z}_d^m$ of $a_1x_1 + a_2x_2 + \dots + a_mx_m \equiv be \pmod{d}$. We claim that $N_b = N_0$ for any $b \in \mathbb{Z}_{d/e}$. Denote by g the greatest common divisor $\gcd(a_1, a_2, \dots, a_m)$. Then one can find integers u_1, u_2, \dots, u_m such that $a_1u_1 + a_2u_2 + \dots + a_mu_m = g$. Since $\gcd(g, d) = e$, we can find c such that $cg \equiv e \pmod{d}$. Thus, $a_1(cu_1) + a_2(cu_2) + \dots + a_m(cu_m) = cg \equiv e \pmod{d}$. If $\mathbf{u} \in \mathbb{Z}_d^m$ is a solution of $a_1x_1 + a_2x_2 + \dots + a_mx_m \equiv 0 \pmod{d}$, then $\mathbf{v} + (bcu_1, bcu_2, \dots, bcu_m)$ is a solution of $a_1x_1 + a_2x_2 + \dots + a_mx_m \equiv b \pmod{d}$. This implies that $N_0 \leq N_b$. On the other hand, if $\mathbf{v} \in \mathbb{Z}_d^m$ is a solution of $a_1x_1 + a_2x_2 + \dots + a_mx_m \equiv b \pmod{d}$, then $\mathbf{v} - (bcu_1, bcu_2, \dots, bcu_m)$ is a solution of $a_1x_1 + a_2x_2 + \dots + a_mx_m \equiv 0 \pmod{d}$. This implies that $N_b \leq N_0$. Now we have $d^m = \sum_{b \in \mathbb{Z}_d} N_b = \frac{d}{e} \times N_0$. The desired result follows. \square

Based on Lemma 1, we first provide a construction of k -uniform quantum state through symmetric matrices. Our map φ is in fact a quadratic function. Let ζ_d denote a d th primitive root of unity in \mathbb{C} . For two subsets $A, B \subseteq \{1, 2, \dots, n\}$ and a matrix $H = (h_{ij}) \in \mathbb{M}_{n \times n}(\mathbb{Z}_d)$, we denote by $H_{A \times B}$ the submatrix $(h_{ij})_{i \in A, j \in B}$. An $n \times n$ matrix E over \mathbb{Z}_d is called invertible if there exists an $n \times n$ matrix G over \mathbb{Z}_d such that $EG = GE$ is equal to the identity matrix. It is well known that E is invertible if and only if the determinate of E is co-prime with d .

If E is invertible, then for any nonzero vector $\mathbf{c} \in \mathbb{Z}_d^n$, we must have $\mathbf{c}E \neq \mathbf{0}$. Otherwise, one would have $\mathbf{0} = \mathbf{0}E^{-1} = \mathbf{c}EE^{-1} = \mathbf{c}$.

Theorem 3. *If there is a zero diagonal symmetric matrix $H \in \mathbb{M}_{n \times n}(\mathbb{Z}_d)$ such that for any subset A of $\{1, 2, \dots, n\}$ with $|A| = k$, there exists a subset B of A with $|B| = k$ such that the submatrix $H_{A \times B}$ is a $k \times k$ invertible matrix over \mathbb{Z}_d , then the n -qudit state $|\Phi\rangle = \sum_{\mathbf{c} \in \mathbb{Z}_d^n} \varphi(\mathbf{c})|\mathbf{c}\rangle$ is k -uniform with $\varphi(\mathbf{c}) = \zeta_d^{\tilde{H}\mathbf{c}^T}$, where $\tilde{H} = (\tilde{h}_{ij})$ with $\tilde{h}_{ij} = h_{ij}$ for $i < j$ and 0 otherwise.*

Proof. Consider the map f from \mathbb{Z}_d^n to \mathbb{Z}_d^n given by $f(\mathbf{c}) = \mathbf{c}\tilde{H}\mathbf{c}^T$. Then for every subset A of $\{1, 2, \dots, n\}$ with $|A| = k$, we have

$$\begin{aligned}f(\mathbf{c}_A, \mathbf{c}_{\bar{A}}) &= \mathbf{c}_A(\tilde{H}_{A \times \bar{A}} + \tilde{H}_{\bar{A} \times A}^T)\mathbf{c}_{\bar{A}}^T + \mathbf{c}_A\tilde{H}_{A \times A}\mathbf{c}_A^T + \mathbf{c}_{\bar{A}}\tilde{H}_{\bar{A} \times \bar{A}}\mathbf{c}_{\bar{A}}^T \\ &= \mathbf{c}_A H_{A \times \bar{A}}\mathbf{c}_{\bar{A}}^T + \mathbf{c}_A \tilde{H}_{A \times A}\mathbf{c}_A^T + \mathbf{c}_{\bar{A}} \tilde{H}_{\bar{A} \times \bar{A}}\mathbf{c}_{\bar{A}}^T.\end{aligned}$$

Hence,

$$\begin{aligned}f(\mathbf{c}_A, \mathbf{c}_{\bar{A}}) - f(\mathbf{c}'_A, \mathbf{c}_{\bar{A}}) &= (\mathbf{c}_A - \mathbf{c}'_A)H_{A \times \bar{A}}\mathbf{c}_{\bar{A}}^T + \mathbf{c}_A\tilde{H}_{A \times A}\mathbf{c}_A^T - \mathbf{c}'_A\tilde{H}_{A \times A}(\mathbf{c}'_A)^T.\end{aligned}$$

If $\mathbf{c}_A = \mathbf{c}'_A$, one has

$$\begin{aligned}\sum_{\mathbf{c}_{\bar{A}} \in \mathbb{Z}_d^{n-k}} \overline{\varphi(c_A, c_{\bar{A}})} \varphi(c'_A, c_{\bar{A}}) &= \sum_{\mathbf{c}_{\bar{A}} \in \mathbb{Z}_d^{n-k}} \zeta_d^{f(\mathbf{c}_A, \mathbf{c}_{\bar{A}})} \zeta_d^{-f(\mathbf{c}_A, \mathbf{c}_{\bar{A}})} \\ &= d^{n-k} = \frac{\langle\Phi|\Phi\rangle}{d^k}.\end{aligned}$$

Note that $\langle\Phi|\Phi\rangle = d^n$.

If $\mathbf{c}_A \neq \mathbf{c}'_A$, then $(\mathbf{c}_A - \mathbf{c}'_A)H_{A \times B}$ is not the zero vector and hence $(\mathbf{c}_A - \mathbf{c}'_A)H_{A \times \bar{A}}$ (denoted by $(a_1, a_2, \dots, a_{n-k})$) is a nonzero vector in \mathbb{Z}_d^{n-k} . Let e be $\gcd(a_1, a_2, \dots, a_{n-k}, d)$. Then $e < d$. By Lemma 2, $(\mathbf{c}_A - \mathbf{c}'_A)H_{A \times \bar{A}}\mathbf{x} = be$ has exactly ed^{n-k-1} solutions in \mathbb{Z}_d^{n-k} for every $b \in \mathbb{Z}_{d/e}$. Hence, by (1), we have

$$\begin{aligned}\sum_{\mathbf{c}_{\bar{A}} \in \mathbb{Z}_d^{n-k}} \overline{\varphi(c_A, c_{\bar{A}})} \varphi(c'_A, c_{\bar{A}}) &= \zeta_d^g \sum_{\mathbf{c}_{\bar{A}} \in \mathbb{Z}_d^{n-k}} \zeta_d^{(\mathbf{c}_A - \mathbf{c}'_A)H_{A \times \bar{A}}\mathbf{c}_{\bar{A}}} \\ &= ed^{n-k-1} \zeta_d^g \sum_{b=0}^{d/e-1} \zeta_d^{be} = 0,\end{aligned}$$

where $g = \mathbf{c}_A\tilde{H}_{A \times A}\mathbf{c}_A^T - \mathbf{c}'_A\tilde{H}_{A \times A}(\mathbf{c}'_A)^T$. This completes the proof. \square

If d is a prime p , then the condition in Theorem 3 can be simplified.

Theorem 4. *Let p be a prime. If there is a zero diagonal symmetric matrix $H \in \mathbb{M}_{n \times n}(\mathbb{Z}_p)$ such that for any subset A of $\{1, 2, \dots, n\}$ with $|A| = k$, the submatrix $H_{A \times \bar{A}}$ has rank k , then the n -qudit state $|\Phi\rangle = \sum_{\mathbf{c} \in \mathbb{Z}_p^n} \varphi(\mathbf{c})|\mathbf{c}\rangle$ is k -uniform with $\varphi(\mathbf{c}) = \zeta_p^{\tilde{H}\mathbf{c}^T}$, where $\tilde{H} = (\tilde{h}_{ij})$ with $\tilde{h}_{ij} = h_{ij}$ for $i < j$ and 0 otherwise.*

Proof. In this case, $H_{A \times \bar{A}}$ has an invertible submatrix $H_{A \times B}$ for some subset B of \bar{A} with $|B| = k$. The desired result follows from Theorem 3. \square

Example 2. Based on Theorem 3, we provide two examples for 1-uniform 2-qudit quantum states, with level 4 and the other with level 6. In both cases, the matrix is given by

$$H = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

The quantum state of level 4 corresponding to this matrix is

$$|\Phi\rangle = |00\rangle + |10\rangle + |20\rangle + |30\rangle + |01\rangle + i|11\rangle - |21\rangle - i|31\rangle \\ + |02\rangle - |12\rangle + |22\rangle - |32\rangle + |03\rangle - i|13\rangle - |23\rangle + i|33\rangle$$

The quantum state of level 6 corresponding to this matrix is

$$|\Phi\rangle = |00\rangle + |10\rangle + |20\rangle + |30\rangle + |40\rangle + |50\rangle + |01\rangle + \zeta_6|11\rangle \\ + \zeta_6^2|21\rangle + \zeta_6^3|31\rangle + \zeta_6^4|41\rangle + \zeta_6^5|51\rangle + |02\rangle + \zeta_6^2|12\rangle + \zeta_6^4|22\rangle \\ + |32\rangle + \zeta_6^2|42\rangle + \zeta_6^4|52\rangle + |03\rangle + \zeta_6^3|13\rangle + |23\rangle + \zeta_6^3|33\rangle \\ + |43\rangle + \zeta_6^3|53\rangle + |04\rangle + \zeta_6^4|14\rangle + \zeta_6^2|24\rangle + |34\rangle + \zeta_6^4|44\rangle \\ + \zeta_6^2|54\rangle + |05\rangle + \zeta_6^5|15\rangle + \zeta_6^4|25\rangle + \zeta_6^3|35\rangle + \zeta_6^2|45\rangle + \zeta_6|55\rangle$$

The second construction applies Lemma 1 to linear codes with good minimum distance and dual distance. As our classical codes are defined over prime fields \mathbb{Z}_p , we consider level p only for primes p for the following construction.

Theorem 5. *If C is a p -ary linear code of length n . Let d and d^\perp be the minimum distance of C and its Euclidean dual C^\perp , respectively. If $\min\{d, d^\perp\} \geq k+1$, then $|\Phi\rangle = \frac{1}{\sqrt{|C|}} \sum_{\mathbf{c} \in C} |\mathbf{c}\rangle$ is k -uniform n -qudit quantum state of level p .*

Proof. It is clear that $\langle \Phi | \Phi \rangle$ is equal to 1. Define the map φ from \mathbb{Z}_p^n to \mathbb{C} given by $\varphi(\mathbf{x}) = 1/\sqrt{|C|}$ if $\mathbf{x} \in C$ and 0 otherwise. Consider a subset A of $\{1, 2, \dots, n\}$ with $|A| = k$.

Since $d^\perp \geq k+1$, for every $\mathbf{c}_A \in \mathbb{Z}_p^k$ there are exactly $|C|/p^k$ vectors $\mathbf{c}_{\bar{A}} \in \mathbb{Z}_p^{n-k}$ such that $(\mathbf{c}_A, \mathbf{c}_{\bar{A}}) \in C$. Thus, If $\mathbf{c}_A = \mathbf{c}'_A$, one has

$$\sum_{\mathbf{c}_{\bar{A}} \in \mathbb{Z}_p^{n-k}} \overline{\varphi(\mathbf{c}_A, \mathbf{c}_{\bar{A}})} \varphi(\mathbf{c}'_A, \mathbf{c}_{\bar{A}}) = \sum_{(\mathbf{c}_A, \mathbf{c}_{\bar{A}}) \in C} \frac{1}{|C|} \\ = \frac{|C|/p^k}{|C|} = \frac{\langle \Phi | \Phi \rangle}{p^k}.$$

If $\mathbf{c}_A \neq \mathbf{c}'_A$, then the Hamming distance between $(\mathbf{c}_A, \mathbf{c}_{\bar{A}})$ and $(\mathbf{c}'_A, \mathbf{c}_{\bar{A}})$ is at most k . This implies that $(\mathbf{c}_A, \mathbf{c}_{\bar{A}})$ and $(\mathbf{c}'_A, \mathbf{c}_{\bar{A}})$ do not belong to C simultaneously for any $\mathbf{c}_{\bar{A}} \in \mathbb{Z}_p^{n-k}$. In other words, $\overline{\varphi(\mathbf{c}_A, \mathbf{c}_{\bar{A}})} \varphi(\mathbf{c}'_A, \mathbf{c}_{\bar{A}}) = 0$ for any $\mathbf{c}_{\bar{A}} \in \mathbb{Z}_p^{n-k}$. In this case, we have $\sum_{\mathbf{c}_{\bar{A}} \in \mathbb{Z}_p^{n-k}} \overline{\varphi(\mathbf{c}_A, \mathbf{c}_{\bar{A}})} \varphi(\mathbf{c}'_A, \mathbf{c}_{\bar{A}}) = 0$. The desired result follows from Lemma 1. \square

Remark 1. (i) In general, the construction in Theorems 3 and Theorems 4 gives better results than the one in Theorem 5. We will see this in Sections 3 and 4.

(ii) For the construction in Theorem 5, we require linear codes with both good minimum distance and dual distance. Algebraic geometry codes provide an excellent family of codes with good minimum distance and dual distance [30]. We will illustrate examples by algebraic geometry codes later in this section and the next two sections.

Corollary 6. *If there exists a p -ary $[n, n/2, \geq k+1]$ -self-dual code, then*

(i) *there exists a k -uniform n -qudit quantum state of level p ;*

(ii) *there exists a $(k-1)$ -uniform $(n-1)$ -qudit quantum state of level p .*

Proof. Part (i) follows from Theorem 5 immediately.

For Part (ii), let C be a p -ary $[n, n/2, \geq k+1]$ -self-dual code. Without loss of generality, we may assume that there is a codeword \mathbf{c} of C such that the last coordinate is not zero. Let C_1 consist of all codewords of C whose last coordinates are zero. Then C_1 is p -ary linear code of dimension $n/2 - 1$, length n and minimum distance at least $k+1$. Delete the last coordinate of C_1 to obtain a p -ary $[n-1, n/2-1, \geq k+1]$ -linear code C_2 . It is clear that the dual code C_2^\perp is the code obtained from C^\perp by deleting the last coordinate. It is clear that C_2^\perp is a p -ary $[n-1, n/2, \geq k]$ -linear code. Applying Theorem 5 to C_2 gives the desired result of Part (ii). \square

Theorem 5 provides an explicit construction of k -uniform quantum states. We give an example below.

Example 3. Consider the binary $[8, 4, 4]$ -self-dual code C with generator matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Then the 8-qudit state $|v\rangle = \frac{1}{4}(|00000000\rangle + |11111111\rangle + |110000111\rangle + |01001011\rangle + |00101101\rangle + |00011110\rangle + |11001100\rangle + |10101010\rangle + |10011001\rangle + |01100110\rangle + |01010101\rangle + |00110011\rangle + |11100010\rangle + |01111000\rangle + |11010001\rangle + |10110100\rangle)$ is 3-uniform.

Remark 2. (i) Self-dual codes have been used to construct k -uniform quantum states in [23, 29]. However, as we remarked, the construction in Theorem 4 gives better results than the one in Theorem 5. Consequently, the construction in Theorem 4 gives better results than those from self-dual codes.

- (ii) In fact, Theorem 5 does not require codes to be self-dual. We now give an example showing that Theorem 5 can give a better k -uniform quantum states than those from self-dual codes. We illustrate this by algebraic geometry codes in the following example.

Example 4. We refer to [30] for background on algebraic curves over finite fields and algebraic geometry codes. It is well known that an algebraic curve over the Galois field $\text{GF}(q)$ of q elements with n rational points and genus g gives a q -ary linear code C with parameters $[n, k, n - k + 1 - g]$ and its dual C^\perp with parameters $[n, n - k, k + 1 - g]$ for any $g \leq k \leq n$.

- (i) By the online table [26], there is an algebraic curve over \mathbb{Z}_5 with 10 rational points and genus 1. Thus, one obtains a 5-ary $[10, 5, 5]$ code C and its dual code C^\perp also has parameters $[10, 5, 5]$. By Theorem 5, one obtains a 4-uniform 10-qudit quantum state of level 5. On the other hand, the optimal 5-ary self-dual code of length 10 has minimum distance 4 (see the online table [28]). Thus, applying Corollary 6 gives only a 3-uniform 10-qudit quantum state of level 5.
- (ii) The above example is not a singularity. We can find other examples showing that Theorem 5 can give better result than Corollary 6. Here is another example. By the online table [26], there is an algebraic curve over \mathbb{Z}_7 with 16 rational points and genus 2. Thus, one obtains a 5-ary $[16, 8, 7]$ code C and its dual code C^\perp also has parameters $[16, 8, 7]$. By Theorem 5, we get a 6-uniform 16-qudit quantum state of level 7. On the other hand, the optimal 7-ary self-dual code of length 16 has minimum distance 6 (see the online table [28]). Thus, applying Corollary 6 gives only a 5-uniform 16-qudit quantum state of level 7.

IV. THE CASE WHERE n IS SMALL

For given d and n , one natural question is what is the maximal k such that there exists a k -uniform n -qudit quantum state of level d . This question motivates the following definition.

Definition 2. For given positive integers $n \geq 2$ and $d \geq 2$, define $k_d(n)$ to be the largest k such that there is an n -qudit state of level d that is k -uniform.

One obvious upper bound on $k_d(n)$ is $n/2$. In this section, we will study some lower bounds on $k_d(n)$ by constructing k -uniform n -qudit quantum states of level d via our results in Section 3. We discuss the cases for small d and large d separately. Although our matrix construction works well for composite levels d , for simplicity we only consider the case where $d = p$ is a prime number.

By Theorem 4, in order to construct a k -uniform quantum state, it is sufficient to find an $n \times n$ zero-diagonal matrix H satisfying that $H_{A \times \bar{A}}$ has rank k for any subset A of $\{1, 2, \dots, n\}$ with $|A| = k$. Through the random matrix counting, we provide a sufficient condition for existence of such a matrix.

Lemma 7. *The number of $n \times n$ zero-diagonal matrices H over \mathbb{Z}_p satisfying that $H_{A \times \bar{A}}$ has rank k for any subset A of $\{1, 2, \dots, n\}$ with $|A| = k$ is at least*

$$p^{\binom{n}{n/2}} \left(1 - \binom{n}{k} \left(1 - \prod_{i=0}^{k-1} \left(1 - \frac{1}{p^{n-k-i}} \right) \right) \right). \quad (1)$$

Proof. Consider the set \mathcal{S} of $n \times n$ zero diagonal symmetric matrices over \mathbb{Z}_p . Then the cardinality of \mathcal{S} is $p^{\binom{n}{2}}$. For a given subset A of $\{1, 2, \dots, n\}$ with $|A| = k$, the set $\{H \in \mathcal{S} : H_{A \times \bar{A}} \text{ is invertible}\}$ has size $\prod_{i=0}^{k-1} (p^{n-k-i} - p^i) \times p^{\binom{n}{2} - k(n-k)}$. This implies that the set $\{H \in \mathcal{S} : H_{A \times \bar{A}} \text{ is not invertible}\}$ has size $p^{\binom{n}{2}} - p^{\binom{n}{2} - k(n-k)} \times \prod_{i=0}^{k-1} (p^{n-k-i} - p^i)$. By the union bound, the number of zero diagonal symmetric matrices H satisfying that, for any subset A of $\{1, 2, \dots, n\}$ with $|A| = k$, $H_{A \times \bar{A}}$ is invertible is at least $p^{\binom{n}{2}} - \binom{n}{k} \left(p^{\binom{n}{2}} - p^{\binom{n}{2} - k(n-k)} \times \prod_{i=0}^{k-1} (p^{n-k-i} - p^i) \right)$. The desired result follows. \square

Corollary 8. *If the triple (n, k, p) satisfies $\binom{n}{k}(p^k - 1) \leq (p - 1)p^{n-k}$, then there exists a k -uniform n -qudit quantum state of level p .*

Proof. Denote by $N_p(n, k)$ the number in (1). By Theorem 4 and Lemma 7, it is sufficient to show that $N_p(n, k) > 0$ under the condition of this Corollary. Indeed

$$\begin{aligned} N_p(n, k) &> p^{\binom{n}{n/2}} \left(1 - \binom{n}{k} \sum_{i=0}^{k-1} \frac{1}{p^{n-k-i}} \right) \\ &= p^{\binom{n}{n/2}} \left(1 - \binom{n}{k} \times \frac{1}{p^{n-k}} \times \frac{p^k - 1}{p - 1} \right) \geq 0. \end{aligned}$$

This completes the proof. \square

A. Small k

In [29], it was proved that for any $n \geq 5$, there exists a 2-uniform n -qudit quantum state of level 2. By using the above corollary, we can extend this results largely. For instance, we have the following result.

Theorem 9. *For any prime p , there exists an integer M_k such that for any $n \geq M_k$, one can construct a k -uniform n -qudit of level p . Furthermore, one has the following quantum states.*

- (i) *For any $n \geq 8$ and integer $k \geq 1$, there exists a 3-uniform n -qudit quantum state of level p .*

- (ii) For any $n \geq 12$, there exists a 4-uniform n -qudit quantum state of level p .
- (iii) For any $n \geq 18$, there exists a 5-uniform n -qudit quantum state of level p .

Proof. Recall that $N_p(n, k)$ denotes the number in (1). We also note that for fixed n and k , $N_p(n, k)$ monotonically decreases when p increases. By Corollary 8, for a fixed k , $N_2(n, k) > 0$ for all sufficiently large n , i.e., there exists an integer M_k such that $N_2(n, k) > 0$ for any $n \geq M_k$. Hence, $N_p(n, k) > 0$ for any $p \geq 2$ and $n \geq M_k$. This completes the proof for the first part.

A simple calculation shows that $N_2(n, 3) > 0$ for all $n \geq 12$, $N_p(n, 3) > 0$ for all $n \geq 8$. By computer search, we find that $k_n(2) \geq 3$ for $8 \leq n \leq 11$ (see Table I below). This completes the proof of Part (i).

The similar arguments apply to the proof of Parts (ii) and (iii). \square

B. $p = 2, 3, 5, 7$

Through computer search, we are able to find some lower bounds on $k_d(n)$. Due to our computation limitation, n is limited to 24 or smaller. Table I provides lower bounds on $k_p(n)$ via construction of Theorem 4. The entries with “-” in Table I means that our computation limit does not allow us to find a reasonable lower bound on the corresponding $k_p(n)$.

Table I

n	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
$k_2(n)$	1	1	1	2	3	2	3	3	3	3	4	4	4	4	4	4
$k_3(n)$	1	1	2	2	3	3	3	3	4	4	4	4	5	5	5	5
$k_5(n)$	1	1	2	2	3	3	3	4	4	4	5	5	5	5	6	6
$k_7(n)$	1	1	2	2	3	3	3	4	4	4	5	5	5	6	6	7
n	18	19	20	21	22	23	24									
$k_2(n)$	5	5	5	5	5	5	6									
$k_3(n)$	5	5	-	-	-	-	-									
$k_5(n)$	6	-	-	-	-	-	-									
$k_7(n)$	7	-	-	-	-	-	-									

Table I provides lower bounds $k_p(n)$ only for prime levels p . As our Theorem 3 works well for composite levels d , we give another table showing lower bounds $k_d(n)$ for $d = 4, 6, 8$ and 9. Due to our computation limitation, we compute $k_d(n)$ only up to $n = 10$.

Table II

n	2	3	4	5	6	7	8	9	10
$k_4(n)$	1	1	1	2	3	2	3	3	3
$k_6(n)$	1	1	1	2	3	2	3	3	3
$k_8(n)$	1	1	1	2	3	2	3	3	3
$k_9(n)$	1	1	2	2	3	3	3	3	4

In addition, we provide one matrix that gives a 3-uniform 6-qudit quantum states of level 2. As our construction in Theorem 4 is explicit, the quantum state can

be explicitly written down as long as the corresponding matrix is known.

$$\begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \end{pmatrix}$$

The corresponding quantum state for the above matrix is

$$\begin{aligned} |\Phi\rangle = & |000000\rangle + |100000\rangle + |010000\rangle - |110000\rangle + |001000\rangle \\ & - |101000\rangle + |011000\rangle + |111000\rangle + |000100\rangle - |100100\rangle \\ & - |010100\rangle - |110100\rangle - |001100\rangle - |101100\rangle + |011100\rangle \\ & - |111100\rangle + |000010\rangle + |100010\rangle + |010010\rangle - |110010\rangle \\ & - |001010\rangle + |101010\rangle - |011010\rangle - |111010\rangle - |000110\rangle \\ & + |100110\rangle + |010110\rangle + |110110\rangle - |001110\rangle - |101110\rangle \\ & + |011110\rangle - |111110\rangle + |000001\rangle + |100001\rangle - |010001\rangle \\ & + |110001\rangle + |001001\rangle - |101001\rangle - |011001\rangle - |111001\rangle \\ & - |000101\rangle + |100101\rangle - |010101\rangle - |110101\rangle + |001101\rangle \\ & + |101101\rangle + |011101\rangle - |111101\rangle - |000011\rangle - |100011\rangle \\ & + |010011\rangle - |110011\rangle + |001011\rangle - |101011\rangle - |011011\rangle \\ & - |111011\rangle - |000111\rangle + |100111\rangle - |010111\rangle - |110111\rangle \\ & - |001111\rangle - |101111\rangle - |011111\rangle + |111111\rangle \end{aligned}$$

The following Table III shows lower bounds on $k_d(n)$ via our Corollary 6 and Theorem 5. Some of entries in Table III are obtained via Corollary 6 from those best-known self-dual codes in the online table [28], while some others are obtained from Theorem 5 through algebraic geometry codes and computer search. In particular, all entries for $p = 7$ are obtained from algebraic geometry codes. Note that in Table III some entries on $k_p(n)$ for odd n are computed from Corollary 6(ii).

Table III

n	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
$k_2(n)$	1	1	1	1	2	2	3	2	2	2	3	2	3	3	3	3
$k_3(n)$	1	1	2	2	2	2	2	2	3	4	5	3	3	4	5	4
$k_5(n)$	1	1	2	2	3	2	3	3	4	4	5	4	5	5	6	5
$k_7(n)$	1	1	2	2	3	3	4	3	4	4	5	5	5	5	6	5
n	18	19	20	21	22	23	24									
$k_2(n)$	3	3	3	4	5	6	7									
$k_3(n)$	4	4	5	5	6	7	8									
$k_5(n)$	6	6	7	6	7	7	8									
$k_7(n)$	6	7	8	6	7	7	8									

Remark 3. Comparing Tables I with III, we find that Theorem 4 usually gives the same or better results than Theorem 5. The only exceptional cases are $k_2(24)$ and $k_7(8)$. This is due to the extreme example of binary Golay [24, 12, 8]-self-dual code and MDS code \mathbb{Z}_7 .

C. Large level p

The main purpose of this subsection is to prove that, for any given even n , we have $k_p(n) = n/2$ for sufficiently large prime p .

Theorem 10. *For any given even integer $n \geq 2$, if an odd prime p satisfies $p \geq \binom{n}{n/2} + 1$, then $k_p(n) = n/2$.*

Proof. By Theorem 4 and Lemma 7, it is sufficient to show that $N_p(n, n/2) > 0$ under the condition of our theorem. Indeed

$$\begin{aligned} N_p(n, n/2) &= p^{\binom{n}{n/2}} \left(1 - \binom{n}{n/2} \left(1 - \prod_{i=1}^{n/2} \left(1 - \frac{1}{p^i} \right) \right) \right) \\ &\geq p^{\binom{n}{n/2}} \left(1 - \binom{n}{n/2} \sum_{i=1}^{n/2} \frac{1}{p^i} \right) \\ &> p^{\binom{n}{n/2}} \left(1 - \frac{\binom{n}{n/2}}{p-1} \right). \end{aligned}$$

If $p \geq \binom{n}{n/2} + 1$, then $1 - \frac{\binom{n}{n/2}}{p-1} \geq 0$ and hence $N_p(n, n/2) > 0$. The desired result follows. \square

V. THE CASE WHERE n IS LARGE

For a fixed $d \geq 2$, to see how $k_d(n)$ varies as n tends to infinity, we define the following asymptotic quantity.

Definition 3. For a given integer $d \geq 2$, define the asymptotic quantity

$$\lambda_d = \limsup_{n \rightarrow \infty} \frac{k_d(n)}{n}.$$

Obviously, $\lambda_d \leq 1/2$. Again, we will study some lower bounds on λ_d by constructing k -uniform n -qudit quantum states of level d via our results in Section 3. In addition, we give existence bounds and constructive bounds on λ_d separately. As one can expect, constructive bounds are usually worse than existence bounds.

A. Existence bounds on λ_p

We first provide an existence bound via Lemma 7. For any integer $d \geq 2$, the d -ary entropy function is defined by

$$H_d(x) := x \log_d(d-1) - x \log_d x - (1-x) \log_d(1-x).$$

By Stirling's formula, we have

$$\lim_{n \rightarrow \infty} \frac{\log_2 \binom{n}{k}}{n} = H_2(\lambda) \quad \text{if } \frac{k}{n} \rightarrow \lambda.$$

Theorem 11. *Let λ be a root of the equation $H_2(x) = (1-2x) \log_2 p$. Then $\lambda_p \geq \lambda$.*

Proof. Choose a very small $\varepsilon \in (0, \lambda)$. Put $k = \lfloor (\lambda - \varepsilon)n \rfloor$. By Theorem 4 and Lemma 7, if we can show that $N_p(n, k) > 0$, there exists a k -uniform n -qudit quantum state of level d . Note that

$$\begin{aligned} N_p(n, k) &= p^{\binom{n}{n/2}} \left(1 - \binom{n}{k} \left(1 - \prod_{i=1}^k \left(1 - \frac{1}{p^{n-k-i}} \right) \right) \right) \\ &\geq p^{\binom{n}{n/2}} \left(1 - \binom{n}{k} p^{-n+2k} \sum_{i=1}^k \frac{1}{p^i} \right) \\ &> p^{\binom{n}{n/2}} \left(1 - \frac{\binom{n}{k} p^{-n+2k}}{p-1} \right). \end{aligned}$$

If

$$p \geq \binom{n}{k} p^{-n+2k} + 1, \quad (2)$$

then $N_p(n, k) > 0$. Since

$$(1 - 2(\lambda - \varepsilon)) \log_p - H_2(\lambda - \varepsilon) > 0, \quad (3)$$

the equation (3) holds for sufficiently large n . This implies that $\lambda_p \geq \lambda - \varepsilon$ for any small ε . Letting ε tend to 0 gives the desired result. \square

Based on Theorem 11, we provide a table for lower bounds on λ_p for small p below.

Table IV

p	2	3	5	7	11	13	17
λ_p	0.1705	0.2461	0.3081	0.3360	0.3634	0.3714	0.3821

Next let us derive a lower bound on λ_p from self-dual codes via Corollary 6.

Theorem 12. *One has*

$$\lambda_p \geq H_p^{-1} \left(\frac{1}{2} \right),$$

where $H_p^{-1}(y)$ is the inverse function of $H_p(x)$.

Proof. By [25], there exists a family of p -ary self-dual code achieving the Gilbert-Vrashamov bound, i.e., there exists a family of p -ary $[n, n/2, \geq k+1]$ -self-dual code such that $\lim_{n \rightarrow \infty} \frac{k}{n} \rightarrow \delta$, where $H_p(\delta) = \frac{1}{2}$, i.e., $\delta = H_p^{-1}(\frac{1}{2})$. It follows immediately that $\lambda_p \geq \delta = H_p^{-1}(\frac{1}{2})$. \square

Based on Theorem 12, we provide a table for lower bounds on λ_p for small p below.

Table V

p	2	3	5	7	11	13	17
λ_p	0.110	0.159	0.210	0.237	0.268	0.278	0.293

Remark 4. Once again, the asymptotic result also shows that our matrix constriction given in Theorem 4 is in general better than the one from self-dual codes given in Theorem 5.

B. Constructive bounds on λ_p

Definition 4. Let p be a prime and let $r \geq 2$ be an integer. A \mathbb{Z}_p -basis $\{\alpha_1, \dots, \alpha_r\}$ of the Galois field $\text{GF}(p^r)$ is called trace-orthogonal if $\text{Tr}(\alpha_i \alpha_j) = 0$ for all $1 \leq i \neq j \leq r$, where Tr is the trace map from $\text{GF}(p^r)$ to \mathbb{Z}_p .

It is well known that there always exists a trace-orthogonal basis of $\text{GF}(p^r)$ over \mathbb{Z}_p [27, Chapter 5]. Note that if $\{\alpha_1, \dots, \alpha_r\}$ is a trace-orthogonal basis of $\text{GF}(p^r)$ over \mathbb{Z}_p , then $\text{Tr}(\alpha_i^2) \neq 0$ for all $1 \leq i \leq r$. Otherwise, one would have $\text{Tr}(\alpha_i x) = 0$ for all $x \in \text{GF}(p^r)$ which is impossible.

Now we fix a trace-orthogonal basis $\{\alpha_1, \dots, \alpha_r\}$ of $\text{GF}(p^r)$ over \mathbb{Z}_p . Let a_i denote $\text{Tr}(\alpha_i^2)$. Then $a_i \in \mathbb{Z}_p \setminus \{0\}$. Thus, every element β of $\text{GF}(p^r)$ can be written as a linear combination $\beta = \sum_{i=1}^r b_i \alpha_i$ with $b_i \in \mathbb{Z}_p$. We denote by $\pi(\alpha)$ and $\pi^\perp(\alpha)$ the vectors $(b_1, b_2, \dots, b_r) \in \mathbb{Z}_p^r$ and $(a_1 b_1, a_2 b_2, \dots, a_r b_r) \in \mathbb{Z}_p^r$, respectively. Extend π and π^\perp to the maps from $\text{GF}(p^r)^n$ to \mathbb{Z}_p^{rn} given by

$$\begin{aligned} \pi(u_1, u_2, \dots, u_n) &= (\pi(u_1), \pi(u_2), \dots, \pi(u_n)); \\ \pi^\perp(u_1, u_2, \dots, u_n) &= (\pi^\perp(u_1), \pi^\perp(u_2), \dots, \pi^\perp(u_n)). \end{aligned}$$

Lemma 13. Let C be a linear code of length n over $\text{GF}(p^r)$. If C^\perp is the dual code of C , then $\pi^\perp(C^\perp)$ is the dual code of $\pi(C) \in \mathbb{Z}_p^{rn}$.

Proof. Let $\mathbf{u} = (u_1, u_2, \dots, u_n) \in C$ and $\mathbf{v} = (v_1, v_2, \dots, v_n) \in C^\perp$. Then we have

$$\begin{aligned} 0 &= \text{Tr} \left(\sum_{i=1}^n u_i v_i \right) = \sum_{i=1}^n \sum_{j=1}^r \sum_{\ell=1}^r u_{ij} v_{i\ell} \text{Tr}(\alpha_j \alpha_\ell) \\ &= \sum_{i=1}^n \sum_{j=1}^r u_{ij} v_{ij} a_j = \pi(\mathbf{u}) \cdot \pi^\perp(\mathbf{v}). \end{aligned}$$

This means that $\pi(C)$ and $\pi^\perp(C^\perp)$ are orthogonal. Furthermore, it is easy to see that the sum of their dimensions over \mathbb{Z}_p is rn . This completes the proof. \square

It is a well-known result from algebraic geometry codes that, for any prime power q , there exists a family of q^2 -ary $[n, n/2, \geq k+1]$ codes $\{C\}$ such that C^\perp also have the same parameters $[n, n/2, \geq k+1]$ and $\lim_{n \rightarrow \infty} \frac{k}{n} = \frac{1}{2} - \frac{1}{q-1}$ (see [30]). Furthermore, this family can be constructed in polynomial times.

Theorem 14. For any $p \geq 5$, one has a constructive lower bound on λ_p given by

$$\lambda_p \geq \frac{1}{4} - \frac{1}{2(p-1)}.$$

Proof. Consider a family of p^2 -ary $[n, n/2, \geq k+1]$ codes $\{C\}$ such that C^\perp also have the same parameters $[n, n/2, \geq k+1]$ and $\lim_{n \rightarrow \infty} \frac{k}{n} = \frac{1}{2} - \frac{1}{p-1}$. Consider a trace-orthogonal basis of $\text{GF}(p^2)$ over \mathbb{Z}_p and associated maps π and π^\perp defined in (4). Then both $\pi(C)$ and

$\pi^\perp(C^\perp)$ are p -ary $[2n, n, \geq k+1]$ -linear code. By Theorem 5, we have a k -uniform rn -qudit quantum state of level p . This gives $\lambda_p \geq \lim_{n \rightarrow \infty} \frac{k}{2n} = \frac{1}{4} - \frac{1}{2(p-1)}$. This completes the proof. \square

When p is small, the bound given in Theorem 14 can be further improved by considering algebraic geometry codes over larger extension $\text{GF}(p^{2t})$ for $t \geq 2$.

Theorem 15. For any $t \geq 2$, one has a constructive lower bound on λ_p given by

$$\lambda_p \geq \frac{1}{2t} \left(\frac{1}{2} - \frac{1}{p^t - 1} \right).$$

Proof. The proof is almost identical to the one of Theorem 14 except we consider algebraic geometry codes over larger extension.

Consider a family of p^{2t} -ary $[n, n/2, \geq k+1]$ codes $\{C\}$ such that C^\perp also have the same parameters $[n, n/2, \geq k+1]$ and $\lim_{n \rightarrow \infty} \frac{k}{n} = \frac{1}{2} - \frac{1}{p^t - 1}$. Consider a trace-orthogonal basis of $\text{GF}(p^{2t})$ over \mathbb{Z}_p and associated maps π and π^\perp defined in (4). Then both $\pi(C)$ and $\pi^\perp(C^\perp)$ are p -ary $[2tn, tn, \geq k+1]$ -linear code. By Theorem 5, we have a k -uniform $2tn$ -qudit quantum state of level p . This gives $\lambda_p \geq \lim_{n \rightarrow \infty} \frac{k}{2tn} = \frac{1}{2t} \left(\frac{1}{2} - \frac{1}{p^t - 1} \right)$. This completes the proof. \square

Finally, we provide a table for constructive lower bounds on λ_p for primes $p = 2, 3, 5, \dots, 23$. Note that the value t to obtain the optimal lower bound in Theorem 5 may vary as p varies.

Table V

p	2	3	5	7	11	13	17
λ_p	0.060	0.094	0.125	0.167	0.2	0.208	0.219
t	3	2	1	1	1	1	1

ACKNOWLEDGMENTS

Keqing Feng is supported by NSFC No.11471178,11571007 and the Tsinghua National Lab. on Information Science and Technology. Lingfei Jin is supported in part by Shanghai Sailing Program under the grant 15YF1401200 and by National Natural Science Foundation of China under Grant 11501117. Chaoping Xing and Chen Yuan are supported by the Singapore Ministry of Education Tier 1 under Grant RG20/13.

Appendix A: An example for k -uniform from symmetric matrix

In this appendix, we provide one more matrix that gives a 3-uniform 8-qudit quantum states of level 2. Thus,

the quantum states can be explicitly written down as long as the corresponding matrix is provided by Theorem 4.

$$\begin{pmatrix} 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \end{pmatrix}$$

$$\begin{aligned} |\Phi\rangle = & |00000000\rangle + |10000000\rangle + |01000000\rangle - |11000000\rangle \\ & + |00100000\rangle - |10100000\rangle - |01100000\rangle - |11100000\rangle \\ & + |00010000\rangle + |10010000\rangle + |01010000\rangle - |11010000\rangle \\ & - |00110000\rangle + |10110000\rangle + |01110000\rangle + |11110000\rangle \\ & + |00001000\rangle + |10001000\rangle + |01001000\rangle - |11001000\rangle \\ & - |00101000\rangle + |10101000\rangle + |01101000\rangle + |11101000\rangle \\ & - |00011000\rangle - |10011000\rangle - |01011000\rangle + |11011000\rangle \\ & - |00111000\rangle + |10111000\rangle + |01111000\rangle + |11111000\rangle \\ & + |00000100\rangle - |10000100\rangle - |01000100\rangle - |11000100\rangle \\ & + |00100100\rangle + |10100100\rangle + |01100100\rangle - |11100100\rangle \\ & + |00010100\rangle - |10010100\rangle - |01010100\rangle - |11010100\rangle \\ & - |00110100\rangle - |10110100\rangle - |01110100\rangle + |11110100\rangle \\ & - |00001100\rangle + |10001100\rangle + |01001100\rangle + |11001100\rangle \\ & + |00101100\rangle + |10101100\rangle + |01101100\rangle - |11101100\rangle \\ & + |00011100\rangle - |10011100\rangle - |01011100\rangle - |11011100\rangle \\ & + |00111100\rangle + |10111100\rangle + |01111100\rangle - |11111100\rangle \\ & + |00000010\rangle - |10000010\rangle + |01000010\rangle + |11000010\rangle \\ & - |00100010\rangle - |10100010\rangle + |01100010\rangle - |11100010\rangle \\ & + |00010010\rangle - |10010010\rangle + |01010010\rangle + |11010010\rangle \\ & + |00110010\rangle + |10110010\rangle - |01110010\rangle + |11110010\rangle \\ & - |00001010\rangle + |10001010\rangle - |01001010\rangle - |11001010\rangle \\ & - |00101010\rangle - |10101010\rangle + |01101010\rangle - |11101010\rangle \\ & + |00011010\rangle - |10011010\rangle + |01011010\rangle + |11011010\rangle \\ & - |00111010\rangle - |10111010\rangle + |01111010\rangle - |11111010\rangle \\ & + |00000110\rangle + |10000110\rangle - |01000110\rangle + |11000110\rangle \\ & - |00100110\rangle + |10100110\rangle - |01100110\rangle - |11100110\rangle \\ & + |00010110\rangle + |10010110\rangle - |01010110\rangle + |11010110\rangle \\ & + |00110110\rangle - |10110110\rangle + |01110110\rangle + |11110110\rangle \\ & + |00001110\rangle + |10001110\rangle - |01001110\rangle + |11001110\rangle \\ & + |00101110\rangle - |10101110\rangle + |01101110\rangle + |11101110\rangle \\ & - |00011110\rangle - |10011110\rangle + |01011110\rangle - |11011110\rangle \end{aligned}$$

$$\begin{aligned} & + |00111110\rangle - |10111110\rangle + |01111110\rangle + |11111110\rangle \\ & + |00000001\rangle + |10000001\rangle - |01000001\rangle + |11000001\rangle \\ & - |00100001\rangle + |10100001\rangle - |01100001\rangle - |11100001\rangle \\ & - |00010001\rangle - |10010001\rangle + |01010001\rangle - |11010001\rangle \\ & - |00110001\rangle + |10110001\rangle - |01110001\rangle - |11110001\rangle \\ & - |00001001\rangle - |10001001\rangle + |01001001\rangle - |11001001\rangle \\ & - |00101001\rangle + |10101001\rangle - |01101001\rangle - |11101001\rangle \\ & - |00011001\rangle - |10011001\rangle + |01011001\rangle - |11011001\rangle \\ & + |00111001\rangle - |10111001\rangle + |01111001\rangle + |11111001\rangle \\ & - |00000101\rangle + |10000101\rangle - |01000101\rangle - |11000101\rangle \\ & + |00100101\rangle + |10100101\rangle - |01100101\rangle + |11100101\rangle \\ & + |00010101\rangle - |10010101\rangle + |01010101\rangle + |11010101\rangle \\ & + |00110101\rangle + |10110101\rangle - |01110101\rangle + |11110101\rangle \\ & - |00001101\rangle + |10001101\rangle - |01001101\rangle - |11001101\rangle \\ & - |00101101\rangle - |10101101\rangle + |01101101\rangle - |11101101\rangle \\ & - |00011101\rangle + |10011101\rangle - |01011101\rangle - |11011101\rangle \\ & + |00111101\rangle + |10111101\rangle - |01111101\rangle + |11111101\rangle \\ & + |00000011\rangle - |10000011\rangle - |01000011\rangle - |11000011\rangle \\ & + |00100011\rangle + |10100011\rangle + |01100011\rangle - |11100011\rangle \\ & - |00010011\rangle + |10010011\rangle + |01010011\rangle + |11010011\rangle \\ & + |00110011\rangle + |10110011\rangle + |01110011\rangle - |11110011\rangle \\ & + |00001011\rangle - |10001011\rangle - |01001011\rangle - |11001011\rangle \\ & - |00101011\rangle - |10101011\rangle - |01101011\rangle + |11101011\rangle \\ & + |00011011\rangle - |10011011\rangle - |01011011\rangle - |11011011\rangle \\ & + |00111011\rangle + |10111011\rangle + |01111011\rangle - |11111011\rangle \\ & - |00000111\rangle - |10000111\rangle - |01000111\rangle + |11000111\rangle \\ & - |00100111\rangle + |10100111\rangle + |01100111\rangle + |11100111\rangle \\ & + |00010111\rangle + |10010111\rangle + |01010111\rangle - |11010111\rangle \\ & - |00110111\rangle + |10110111\rangle + |01110111\rangle + |11110111\rangle \\ & + |00001111\rangle + |10001111\rangle + |01001111\rangle - |11001111\rangle \\ & - |00101111\rangle + |10101111\rangle + |01101111\rangle + |11101111\rangle \\ & + |00011111\rangle + |10011111\rangle + |01011111\rangle - |11011111\rangle \\ & + |00111111\rangle - |10111111\rangle - |01111111\rangle - |11111111\rangle \end{aligned}$$

- [2] Bennett, C. H., D. P. DiVincenzo, J. Smolin, and W. K. Wootters, 1996, Phys. Rev. A 54, 3824.
- [3] Schumacher, B., 1995, Phys. Rev. A 51, 2738.
- [4] Jozsa, R., 1997, Entanglement and quantum computation, eprint quant-ph/9707034.
- [5] Jozsa, R., and N. Linden, 2002, On the role of entanglement in quantum computational speedup, eprint quant-ph/0201143.
- [6] Virmani, S., S. F. Huelga, and M. B. Plenio, 2005, Phys. Rev. A 71, 042328.
- [7] Koashi, M., and A. Winter, 2004, Phys. Rev. A 69, 022309.
- [8] Gurvits, L, arXiv:quant-ph/0303055v.
- [9] M. Huber, P. Erker, H. Schimpf, A. Gabriel, and B. Hiesmayr, Phys. Rev. A 83, 040301(R).
- [10] M. Huber, F. Mintert, A. Gabriel and B. Hiesmayr Phys. Rev. Lett. 104, 210501 (2010).
- [11] N. Gisin and H. Bechmann-Pasquinucci, Phys. Rev. A 246,1 (1998).
- [12] A. Higuchi and A. Sudbery, Phys. Lett. A 273,213 (2000).
- [13] V. Kendon, K. Nemoto, and W. J. Munro, J. Mod. Opt. 49, 1709 (2002).
- [14] I. Brown, S. Stepney, A. Sudbery, and S. L. Braunstein, J. Phys. A 38, 1119 (2005).
- [15] A. Osterloh and J. Siewert, Int. J. Quantum Inf. 4, 531 (2006).
- [16] A. Borras, A. Plastino, J. Batle, C. Zander, M. Casas and A. Plastino, J. Phys. A 40, 13407 (2007).
- [17] S. Brierley and A. Higuchi, Phys. A 40, 8455(2007).
- [18] J. Martin, O. Giraud, P. Braun, D. Braun and T. Bastin, Phys. Rev. A 81, 062347 (2010).
- [19] S. Tamaryan, A. Sudbery and L. Tamaryan, Phys. Rev. A 81, 052319 (2010).
- [20] P. Facchi, G. Florio, G. Parisi and S. Pascazio, Phys. Rev. A 81, 052319 (2010).
- [21] P. Facchi, G. Florio, U. Marzolino, G. Parisi and S. Pascazio, J. Phys. A 43, 225303 (2010).
- [22] L. Arnaud and N. Cerf, Phys. Rev. A 87, 012319 (2013).
- [23] D. Goyeneche and K. Zyczkowski, Phys. Rev. A 90, 022316(2014).
- [24] A. Higuchi and A. Sudbery, Phys. Lett. A 246, 1(1998).
- [25] F. J. Macwilliams, N. J. Sloane and J. G. Thompson, Discrete Mathematics, 3(1972).
- [26] G. van der Geer, online table at <http://www.manypoints.org>.
- [27] G. L. Mullen and D. Panario, *Handbook of Finite Fields*, Chapman and Hall/CRC, 2013.
- [28] P. Gaborit and A. Otmani, online table at http://www.unilim.fr/pages_perso/philippe.gaborit/SD.
- [29] A. J. Scotte, Phys. Rev. A 69, 052330(2004).
- [30] H. Stichtenoth, *Algebraic Function Fields and Codes*, Universitext, Springer-Verlag, Berlin, 1993.